PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:		)	
		)	
Lawrence Smith et al.		)	Examiner: M. Vaughan
		)	
Serial No.:	09/389,540	)	Group Art Unit: 2131
		)	
Filed:	September 3, 1999	)	Docket: 105.163US1

For: VIRTUAL SMART CARD SYSTEM AND METHOD

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, mailed on October 14, 2004 and received by the USPTO on October 18, 2004, from the Final Rejection of claims 1-17 of the above-identified application, as set forth in the Final Office Action mailed on April 14, 2004.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2). The Appellant respectfully requests consideration and reversal of the Examiner's rejections of pending claims.

APPEAL BRIEF UNDER 37 C.F.R. 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, SECURE COMPUTING CORPORATION, a corporation organized and existing under and by virtue of the laws of the State of Delaware, and having an office and place of business at 2675 Long Lake Road, Roseville, Minnesota 55113, in an assignment recorded on January 31, 2000, (Reel /Frame: 010580/0214).

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 1-17 are pending and stand currently rejected. These seventeen claims are the subject of the present appeal (see the Claims Appendix for a list of the claims on appeal).

4. STATUS OF AMENDMENTS

Claims 1-17 are in the form they were in after the Amendment and Response filed by Appellant on March 1, 2004. The claims listed in the Claims Appendix reflect the claims as they currently exist. No amendments were filed after the final rejection.

5. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellant teaches and claims a public key authentication scheme based on the use of smart cards. Appellant also teaches and claims a public key authentication scheme based on the use of "virtual" smart cards.

Appellant discusses, at p. 2, lines 1-22, the use of public key cryptography to authenticate users securely. Under public key cryptography, a public key/private key pair is assigned to a user. The public key is used by others to encrypt data. The encrypted data can only be read by the owner of the corresponding private key. Although there is no cohesive approach to public key authentication, Appellant notes, at p. 4, line 27- p. 5, line 12, that smart cards can be used effectively to safeguard and transport a user's

credentials under a Public Key Infrastructure (PKI) based public key authentication scheme and describes such a PKI-based public key authentication system.

Appellant teaches, at p. 9, line 7 through p. 10, line 20, and claims in claims 14-16, a public key authentication system which includes an authentication server, a directory service connected to the authentication server, and a host system.

The directory service includes a two or more public keys; each public key is associated with a unique user identifier. The host system includes a public key authentication client and an interface to a smart-card-enabled application.

The public key authentication client is connected to the authentication server. In operation, the public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server. The authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

Appellant also teaches at p. 11, lines 21-26 and claims in claim 15, an authentication server as described above which implements role-based access control.

Furthermore, Appellant teaches at p. 11, line 27- p. 12, line 4 and claims in claim 16, an authentication server as described above which implements automatic logging of authentication attempts.

As Appellant notes at p. 4, line 13 – 17, migration to smart card based public key authentication won't happen overnight. In systems without smart cards, therefore, it was common to store the private key directly on the user's hard drive, protected only by a simple password.

Appellant therefore noted a need for a public key authentication system which is secure and portable, but which can operate with smart cards. Appellant teaches such a system at p. 5, line 22 – p. 8, line 2, and claims in claims 1-9 and 17, a system and method for authenticating users based on "virtual" smart card-based public key authentication.

As noted at p. 6, line 5 – p. 7, line 24, and claimed in claims 1-9 and 17, a virtual smart card agent is connected to a virtual smart card server, which is connected in turn to storage containing two or more virtual smart cards. The virtual smart card agent

authenticates the user using a one-time password and accesses the authenticated user's virtual smart card in storage to obtain the user's private key.

Such an approach provides two-factor authentication and allows the user to transport his or her private key and other smart card data to other systems without the added cost and complexity of deploying smart cards and smart card readers.

Finally, Appellant teaches at p. 8, line 3 – p. 9, line 6 and claims in claims 10-13, a two-factor authentication scheme using a certificate based PKI system. According to the scheme, first and second keys are assigned to each user, wherein the first and second key form a public/private key pair. A digital certificate is issued to the first user, wherein the digital certificate is associated with the second key assigned to the first user.

The user enters a one-time password. The one-time password is encrypted with the first key assigned to the first user to form an encrypted one-time password. A check is made to verify that the digital certificate issued to the first user was signed by a recognized certificate authority and the second key assigned to the first user is accessed using the digital certificate.

The encrypted one-time password is decrypted with the second key associated with the digital certificate to recover the one-time password and the recovered one-time password is compared to an expected one-time password.

Appellant teaches at p. 8, lines 17-27, and claims in claim 12, that the check made to verify the digital certificate includes accessing a CRL to determine if the certificate has been revoked.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

a. Are claims 1-9, and 17 properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Benson (E.P. 0936530) in view of Vilhuber (U.S.P. 6,470,453)?

b. Are claims 10-16 properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of the Handbook of Applied Cryptology by A.J. Menezes?

7. ARGUMENT

Claims 1-9, and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Benson (E.P. 0936530) in view of Vilhuber (U.S.P. 6,470,453).

1) The Applicable Law

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To do that the Examiner must show that some objective teaching in the prior art or some knowledge generally available to one of ordinary skill in the art would lead an individual to combine the relevant teaching of the references. *Id.*

The *Fine* court stated that:

> Obviousness is tested by "what the combined teaching of the references would have suggested to those of ordinary skill in the art." *In re Keller*, 642 F.2d 413, 425, 208 USPQ 871, 878 (CCPA 1981)). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." *ACS Hosp. Sys.*, 732 F.2d at 1577, 221 USPQ at 933. And "teachings of references can be combined *only* if there is some suggestion or incentive to do so." *Id.* (emphasis in original).

The M.P.E.P. adopts this line of reasoning, stating that

> In order for the Examiner to establish a *prima facie* case of obviousness, three base criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.

M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir. 1991)). In addition, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143. The Examiner must avoid hindsight. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566,

1568 (Fed. Cir. 1990). Also, prior art must by considered in its entirety, including disclosures that teach away from the claims. *M.P.E.P. 2141.02.*

2) Applying the Law

a) Discussion of the Rejections of Claims 1-9 and 17.

Benson describes a virtual smart card system. Benson's virtual smart card system derives two symmetric keys from the owner's password. The first key is an authentication key and the second key is a protection key. The authentication key is used to securely identify the owner to the virtual smart card server. The protection key is used to encrypt protected information that the virtual smart card uploads to the virtual smart card server and to decrypt protected information that the virtual smart card downloads from the virtual smart card server. Benson, col. 6, paras. 21 and 22.

Vilhuber describes the use of a one-time password to authenticate a user to a network access server. Col. 8, lines 35-37.

Applicant teaches that one advantage of smart cards is that they provide two-factor authentication. That is, the user proves his identity by presenting something he has (i.e., the card with its private key) and something he knows (i.e., the card's PIN). Applicant contrasts this to simple passwords, which provide only single-factor authentication and are, therefore, "vulnerable to any number of well known password guessing attacks." Specification, p. 5, lines 3-12.

Applicant teaches that one way to approach the stronger protection of two-factor authentication provided by a smart card implementation is to use one-time passwords generated by an authentication token. By implementing a one-time password solution, the user proves his identity by presenting something he has (i.e., the one-time password generated by the authentication token) and something he knows (i.e., the token's PIN). Specification, p. 5, lines 22-28.

Benson does not consider the problem of two-factor authentication. Instead, as noted at [0021] Benson determines two symmetric keys from a simple password. Benson uses the first symmetric key to authenticate the user to a virtual smart card server and the second symmetric key to encrypt protected information stored on the user's virtual smart

card. Although the protected information may include a private key, the private key is not used for interactions with the virtual smart card server.

A one-time password, even one generated without the authentication token, provides additional security over the simple password described by Benson. For one, it is difficult to discover a one-time password. In addition, the authentication function described by Appellant operates independently of the smart card emulation, allowing the system designer to strengthen the authentication piece of the system without impacting the smart card emulation. This contrasts to Benson, who generates and uses an authentication key and a protection key, each calculated from a simple password as part of smart card emulation.

Additionally, Appellants respectfully submit that proper motivation is lacking to combine Benson and Vilhuber. As discussed above, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Appellants are unable to find such a suggestion or motivation in the references to make the combination. The Examiner states, apparently to explain why the combination is proper, that

> Bensons says that one can optionally configure a VSC server to require additional authentication material [0067] and that more complex password information can be used [0086]. Vilhuber teaches a more complex password authentication that is more secure. Vilhuber explicitly teaches that the user enters a one time password which is displayed on a token. In view of this, it would have been obvious for one of ordinary skill in the art at the time of the invention to employ the teachings of Vilhuber within the system of Benson because a simple password is not nearly as secure as using one time passwords.

However, Benson itself does not apparently refer to the desirability of using the type of access information referred to in Vilhuber. Thus, the Examiner's statement appears to be a conclusory statement made with the benefit of impermissible hindsight of the Appellants' application.

Further, Benson teaches away from what is described in Vilhuber. Vilhuber describes "Token caching" to allow multiple connections to be made using a same one-time password. And that to establish [an] additional connection, the user "A"

is not required to enter valid user access information a second time (*see* col. 9, lines 8-38). In contrast, Benson states that an owner can insert a Virtual Smart Card with the effect that the Virtual Smart Card's state changes from idle to in-use, and that after removing the virtual smart card from one machine, the owner can potentially insert the virtual smart card into a different machine. However, the owner cannot insert the virtual smart card in the second machine until the owner removes the virtual smart card from the first machine (col. 3, ¶ 0012). Therefore, Benson teaches away from the additional connections in Vilhuber and proper motivation is apparently lacking within Benson and Vilhuber themselves to make the proposed combination. Further, because Benson teaches away from the additional connections using a one-time password of Vilhuber, Appellants submit that proper motivation is lacking for one of ordinary skill in the art to make the proposed combination of Benson and Vilhuber. Reversal of the rejections and reconsideration of claims 1-9 and 17 is respectfully requested.

b) Discussion of the Rejections of Claims 10-16.

Claims 10-16 were rejected under 35 USC § 103(a) as being unpatentable over Benson (EP 936530) in view of Handbook of Applied Cryptography (hereinafter "HAC").

The Examiner stated that "Benson teaches a method of authenticating users using a one time random password". The section the Examiner cites describes authentication of the Virtual Smart Card process, not authentication of the user as described by Applicant and claimed in claims 10-13. Appellant pointed this out in the response to the First Office Action. The Examiner never acknowledged this point.

Appellant also teaches at p. 11, lines 21-26 and claims in claim 15, an authentication server as described above which implements role-based access control. There is no teaching in either Benson or Vilhuber of an authentication which implements role-based access control.

Furthermore, Appellant teaches at p. 11, line 27- p. 12, line 4 and claims in claim 16, an authentication server as described above which implements automatic logging of authentication attempts. There is no teaching in either Benson or Vilhuber of an authentication which implements automatic logging of authentication attempts.

With regard to claims 14-16, Applicant teaches at p. 9, lines 7-29, and claims in claim 14-16, a system capable of handling multiple forms of authentication, including authentication with actual smart cards. As described by Applicant, the principal components of this architecture are the public key authentication client, the authentication server and an LDAP compliant directory service. During login, the public key authentication client connects to authentication server.

The public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server. The authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

As noted above, Benson bases user authentication on a hash of a simple password, generating an authentication key from a hash of the user's password. The VSC server of Benson is, as the Examiner noted, the authentication server. Benson does not, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are described by Applicant and claimed in claims 14-16.

HSC teaches that public-key techniques can be used for challenge-response based identification. As the Examiner notes, HSC teaches that a user can demonstrate knowledge of his or her private key by digitally signing a challenge with his or her private key. Neither Benson nor HSC, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are described by Applicant and claimed in claims 14-16.

Benson states (col. 11, ¶ 0049) that the VSC server authenticates a Virtual Smart Card with the aid of mobile agents and automatic code generation. That each Virtual Smart Card has a unique authentication function, *f*, that this functions accepts a randomly generated number as input and produces a number as output, and [¶ 0050] that the VSC server generates the two random numbers.

The Examiner asserts in the Office Action that in ¶¶ 0084-0086, Benson teaches

that the user is authenticated and that the Virtual Smart Card (VSC) acts a mediator between the user and the server. However, these paragraphs strengthen Appellants' argument that the section in ¶¶ 0049, 0050 cited by the Examiner describes authentication of the Virtual Smart Card process, not authentication of the user. ¶ 0084 states that the VSC Server mediates to ensure that all authentications are successful. The authentications ¶0084 refers to are the VSC authenticating its own implementation, and that these authentications are *distinct from the owner's authentication* [¶ 0083]. Thus, what is asserted as being a one time random password in ¶¶ 0049, 0050 are actually random numbers passed between the VSC and the VSC server to authenticate the VSC. Appellants are unable to find mention of a one-time password in the "User Authentication" section in ¶¶ 0085, 0086.

Appellant teaches at p. 8, lines 17-27, and claims in claim 12, that the check made to verify the digital certificate includes accessing a CRL to determine if the certificate has been revoked.

With regard to claims 14-16, Appellants teach at p. 9, lines 7-29, and claims in claim 14-16, a system capable of handling multiple forms of authentication, including authentication with actual smart cards. As described by Appellants, the principal components of this architecture are the public key authentication client, the authentication server and an LDAP compliant directory service. During login, the public key authentication client connects to authentication server.

The public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server. The authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

Benson is described above. As noted above, Benson bases user authentication on a hash of a simple password, generating an authentication key from a hash of the user's password. The VSC server of Benson is, as the Examiner noted, the authentication server. Benson does not, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are

described by Appellants and claimed in claims 14-16.

HAC teaches that public-key techniques can be used for challenge-response based identification. As the Examiner notes, HAC teaches that a user can demonstrate knowledge of his or her private key by digitally signing a challenge with his or her private key. Neither Benson nor HAC, however, describe the use of a directory service (such as an LDAP directory service) to store public keys, nor a challenge/response authentication mechanism based on the public keys stored in the directory service, both of which are described by Appellants and claimed in claims 14-16.

8. SUMMARY

The Final Office Action fails to meet its burden of establishing a *prima facie* case of obviousness under 35 U.S.C. § 103. It is respectfully submitted that the claimed invention is not unpatentable in view of the cited art. It is respectfully submitted that claims 1-17 should therefore be allowed. Reversal of the Examiner's rejections of claims 1-17 is respectfully requested.

Respectfully submitted,
LAWRENCE SMITH ET AL.
By their Representatives,
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date May 18, 2005 By Thomas J. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 18th day of May, 2005.

THOMAS F. BRENNAN
Name

Thomas J. Brennan
Signature

CLAIMS APPENDIX

The Claims on Appeal

1. (Rejected) A public key authentication system for use in a computer system having a plurality of users, the system comprising:

a virtual smart card server;

storage connected to the virtual smart card server, wherein the storage includes a plurality of virtual smart cards, wherein each virtual smart card is associated with a user and wherein each smart card includes a private key; and

a virtual smart card agent connected to the virtual smart card server, wherein the virtual smart card agent includes a user authentication interface for use by a user in entering a one-time password, wherein the virtual smart card agent authenticates the user using the one-time password and accesses the authenticated user's virtual smart card to obtain the user's private key.

2. (Rejected) The public key authentication system according to claim 1, wherein the virtual smart card agent includes an interface to a smart-card-enabled application.

3. (Rejected) The public key authentication system according to claim 2, wherein the virtual smart card server performs encryption in response to a remote call from the interface.

4. (Rejected) The public key authentication system according to claim 2, wherein the virtual smart card server performs signing in response to a remote call from the interface.

5. (Rejected) The public key authentication system according to claim 2, wherein the virtual smart card server performs key management functions in response to a remote call from the interface.

6. (Rejected) The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card agent and wherein the virtual smart card agent authenticates the user through interaction with the authentication server.

7. (Rejected) The public key authentication system according to claim 1, wherein the public key authentication system further includes an authentication server connected to the virtual smart card server, wherein the authentication server includes means for authenticating a user using a one-time password authentication token.

8. (Rejected) The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over an agent-server transport layer.

9. (Rejected) The public key authentication system according to claim 1, wherein the virtual smart card agent communicates with the virtual smart card server over a secure TCP/IP session.

10. (Rejected) A method of authenticating users, including a first user, attempting to access a computer system, the method comprising:

assigning first and second keys to each user, wherein the first and second key form a public/private key pair;

issuing a digital certificate to the first user, wherein the digital certificate is associated with the second key assigned to the first user;

entering a one-time password;

encrypting the one-time password with the first key assigned to the first user to form an encrypted one-time password;

verifying that the digital certificate issued to the first user was signed by a recognized certificate authority;

accessing, via the digital certificate, the second key assigned to the first user;

decrypting the encrypted one-time password with the second key associated with the digital certificate to recover the one-time password; and

comparing the one-time password against an expected one-time password.

11. (Rejected) The method according to claim 10, wherein the first key is a private key and the second key is a public key.

12. (Rejected) The method according to claim 10, wherein verifying that the digital certificate issued to the first user was signed by a recognized certificate authority includes accessing a CRL to determine if the certificate has been revoked.

13. (Rejected) A computer-readable medium comprising program code which executes the method of claim 10.

14. (Rejected) A public key authentication system for use in a computer system having a plurality of users, the system comprising:

an authentication server;

a directory service connected to the authentication server, wherein the directory service includes a plurality of public keys, wherein each public key is associated with a unique user identifier; and

a host system, wherein the host system includes a public key authentication client and an interface to a smart-card-enabled application, wherein the public key authentication client is connected to the authentication server;

wherein the public key authentication client receives a challenge issued by the authentication server, signs the challenge with a digital signature representing a user and sends the digital signature of the challenge back to the authentication server; and

wherein the authentication server receives the digital signature of the challenge and verifies the digital signature with a public key retrieved from the directory service.

15. (Rejected) The public key authentication system according to claim 14, wherein the authentication server includes role-based access control.

16. (Rejected) The public key authentication system according to claim 14, wherein the authentication server includes automatic logging of authentication attempts.

17. (Rejected) The method of claim 1, wherein entering a one-time password includes displaying the one-time password on an authentication token.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None